View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

一般論文
受付：2005.9.12
受理：2006.1.12

Microsoft Excel の上に大きな有理数とその演算関数を実現する

野　呂　春　文
日本福祉大学　情報社会科学部

The introduction of BigRational and its arithmetic functions into Microsoft Excel

Harufumi　Noro
Faculty of Social and Information Sciences, Nihon Fukushi University

Abstract: This report explains how to introduce so-called BigRational arithmetics into Microsoft Excel. Here, term BigRational means such rational number that has non-limited digits except for the limit of memory size. A BigRational is represented as a pair of arrays of 10,000-based Long integers in Visual Basic on Microsoft Excel. Operations, such as addition, multiplication, division and so on, are defined as functions written by Visual Basic..

Keywords: Microsoft Excel, Visual Basic, Big Rational, arithmetics

１．はじめに

桁数制限の無い，いわゆる大きな整数BigIntegerをMicrosoft Excelの上に実現する方法は別に報告した．初等整数論や暗号学に関する大部分の問題は，大きな整数によって記述できる．しかし，モジュロ代数に基づく剰余環以外の狭い意味の整数に限ると，負の指数を持つ冪乗が定義できないなどの制約が発生する．また，初等整数論を越えて楕円曲線等を取り扱う代数的整数論，すなわち代数曲線上の有理点の問題に取り組むには有理数の実現が不可欠である[1]．そこで，大きな整数の実現に続いて，それに基づく桁数制限のない大きな有理数BigRationalとその演算関数をMicrosoft Excelの上に実現することを試みたので，それを報告し諸氏の批判とアドバイスを求めることとした．

大きな有理数の応用例として，楕円曲線上の有理点の計算を取り上げる．有理点のうちに整点がいくつあるかという問題はワイルズによるフェルマーの最終予想の証明において決め手となった志村・谷山予想と深く関係している．Microsoft Excelのワークシート上で実際に計算を試みる．

２．大きな有理数の実現

ここでは大きな有理数BigRationalとは，分子・分母ともに桁数制限の無い整数である有理数を意味するものとする．そのとき，分子と分母は既約，すなわちそれらの最小公倍数は１に等しく，符号は分子が持つものとする．したがって分母は常に正の整数である．分母が１に等しい場合は，当然のこととして整数とみなされる．

このような数をMicrosoft Excelの上に実現するには，分子と分母をそれぞれ大きな整数として実現すればよい．その詳細は別報を参照されたい．ここで重要なのはMicrosoft Excelのワークシート上，つまりセルにおけるユーザーインターフェースである．別報したとおり，セルに入力できる整数の桁数は小さく，このような問題には対応できないため，セル上では大きな整数は文字列として表わされる．それと同じように，大きな有理数は

セルの上では文字列として表わされる．その表わし方は，最も自然な表現として，例えば，8119/5741 という形を採用する．有理数の演算関数は，この形で表された有理数の文字列を受け取り，分子と分母として処理を行なう．結果は，再び同じ形の文字列としてセルに表示される．

３．大きな有理数の演算関数

大きな有理数の演算関数が持つべき重要な機能は，大きな整数との混合演算を可能にすることである．すなわち，大きな有理数の演算関数は引き数として大きな有理数の文字列と同様に大きな整数も受け入れねばならない．つまり，演算関数の内部では，大きな整数は分母が１に等しい大きな有理数として取り扱われる．そして出力に際しては，もし分母が１に等しければ冗長な「/1」を取り除いた大きな整数の文字列を出力する必要がある．

3.1　単項演算関数

- BigRatReduce(BigRat) As BigRat：　大きな有理数を引き数に取り，約分し，符号が分子にだけ付くようにした大きな有理数の文字列を返す．分母が１であれば，大きな整数の文字列を返す．大きな整数を引き数に与えると，「/1」の形の大きな有理数を返す．
- BigRatNumerator(BigRat) As BigInt：　大きな有理数を引き数に取り，分子を大きな整数として返す．
- BigRatDenominator(BigRat) As BigInt：　大きな有理数を引き数に取り，分母を大きな整数として返す．定義から常に正の整数である．
- BigRatAbs(BigRat) As BigRat：　大きな有理数を引き数に取り，その絶対値を大きな有理数として返す．
- BigRatNegate(BigRat) As BigRat：　大きな有理数を引き数に取り，その符号を反転した大きな有理数を返す．
- BigRatSign(BigRat) As Long：　大きな有理数を引き数に取り，その符号を Long 型整数値として返す．負なら –1，ゼロなら0，正なら1を返す．

3.2　四則演算関数等の２項演算関数

- BigRatCompare(aBigRat, bBigRat) As Long：２個の大きな有理数を比較し結果を Long型整数値として返す．aBigRat > bBigRat なら1，aBigRat = bBigRat なら0，aBigRat < bBigRat なら –1 ，を返す．
- BigRatAdd(BigRat, BigRat) As BigRat：　大きな有理数の和を計算し，結果を大きな有理数として返す．
- BigRatSub(aBigRat, bBigRat) As BigRat：　大きな有理数の差 aBigRat – bBigRat を計算し，結果を大きな有理数として返す．
- BigRatMul(BigRat, BigRat) As BigRat：　大きな有理数の積を計算し，結果を大きな有理数として返す．
- BigRatSquare(BigRat) As BigRat：　大きな有理数の２乗を計算し，結果を大きな有理数として返す．
- BigRatDiv(aBigRat, bBigRat) As BigRat：大きな有理数の商 aBigRat / bBigRat を計算し，結果を大きな有理数として返す．
- BigRatPow(BigRat, Long) As BigRat：　大きな有理数の冪乗を計算し，結果を大きな有理数として返す．冪指数は Long型の整数に限る．大きな有理数，冪指数とも負の値が許される．

3.3　モジュロ演算関数

有理数のモジュロ演算は整数の場合と異なるところがあり，複数の定義が存在するので，特に説明をくわえる．

整数の場合，モジュロ r = a mod b は，除法の基本アルゴリズム a = b×q + r, 0 ≦ r < |b| を満たす r として定義される．したがって，a < 0 に対して，通常の除法における余りとは異なる値となる．

有理数の場合，a を有理数，b を0でない整数とするとき，モジュロ r = a mod b は次のように定義される．a = m/n とする．ここで，m と n は互いに素である．r は，0 ≦ r < |b| となる整数で，m≡r×n (mod b) を満たすものとする．特に，m=1 のとき，すなわち，1≡r×n (mod b) を満たす整数 r は「モジュロ b における n の乗法逆元」と呼ばれる．

有理数に対するモジュロをこのように定義すると，すべての a と b の組み合わせに関して r = a mod b が存在するわけでは無いことに注意が必要である．a = m/n で見たとき，n と b が互いに素であるときだけ r = a mod b が存在する．

例えば，a = 4/6 b = 32 とする．6と32は互いに素ではないから a mod b が存在しないかに見える．しかし，

a = 4/6 = 2/3 であり a mod b は存在し，r = 22である．

有理数に対するモジュロを a − c が b の倍数になるような0 ≦ c < |b| を満たす有理数 c で定義することもあるが，これはほとんど役立たないので採用しない．[2)]

・BigRatMod(BigRat, BigInt) As BigInt：　上で説明した定義にしたがって BigRat mod BigInt を計算し，結果を大きな整数として返す．

3.4　大きな整数との相互変換関数

・BigIntToBigRat(aBIgInt, bBigInt) As BigRat：　２個の大きな整数から大きな有理数 aBigInt/bBigInt を作って返す．

・BigRatToBigInt(BigRat) As BigInt：　大きな有理数を m/n とするとき，割り算を実行して得られた商を大きな整数として返す．

3.5　乱数生成関数

・BigRatRandom(aLong, bLong) As BigRat：　分子が aLong桁，分母が bLong桁の乱数からなる大きな有理数を返す．

４．応用例

楕円曲線上の有理点を計算してみる．楕円曲線の方程式を y^2 = x^3 + ax + b とし，その上の点を P = (x1, y1)，Q = (x2, y2) とすると，P + Q = (x3, y3)，2P = (x4, y4) は次のように計算できる．

x3 = λ^2 − x1 − x2，y3 = -y1 + λ(x1 − x3) ここで，λ = (y2 − y1)/(x2 − x1)

x4 = λ^2 − 2x1，y4 = -y1 + λ(x1 − x4) ここで，λ = (3x1^2 + a)/(2y1)

例として，y^2 = x^3 − 36x上の点 P = (-3, 9) に対して，2P，4P，... の計算を Microsoft Excel のワークシート上に実現してみる．必要な数式を直接セルに記述するだけである．その際，本報告で説明している関数は，BigRatSign と BigRatCompare以外はすべて入れ子にすることができる．例えば，x4 = λ^2 − 2x1という数式を入れ子にして，BigRatSub(BigRatSquare( ), BigRatMul(“2”，)) と書くことができる．関数の中に直接大きな整数や大きな有理数を記述するときは，ダブルクォーテイションで囲んで「文字列」であることを明示する．

唯一，注意すべき点は，曲線のパラメータと初期値を入力するセルに対して，あらかじめセルの書式設定機能を用いて「文字列」指定しておくことである．

計算結果の一部を示すと，2P = (25/4, -35/8) 4P = (1442401/19600,17 2655 6399/274 4000) 8P = (4 3863 0361 8090 1125 6384 9601/2337 1016 4715 9432 2055 8400, 8 7043 6910 9085 5808 2827 5935 6506 2625 4401/1129 8385 8512 4636 1973 7216 6844 9644 8000) である．次の16P では，x の分子・分母の桁数が99桁/98桁，y の分子・分母の桁数が148桁/147桁であった．急速に桁数が大きくなることが特徴である．

５．おわりに

Microsoft Excel上に桁数制限の無い大きな有理数とその演算関数を実現した．別報した大きな整数とあわせれば，初等整数論から代数的整数論，そして，それらに基づく暗号学に関する計算の多くをワークシート上で試すことができる．初学者の教育や学習に使うのみでなく，極めて難解複雑な数論的アルゴリズムを目で確認しながら調べることにも使える．そこから出発して，GAP や Java の BigIntegerクラスライブラリー等を使った本格的な研究に進むこともできるであろう．

文献

（報告の性質上，個々の原著論文は示さず，まとまった著作物をとりあげている．また，訳書がある場合は，それを優先して示した．）

1) Silverman, J.H. and Tate, J.，足立恒雄・木田雅成・小松啓一・田谷久雄訳：楕円曲線論入門．シュプリンガー・フェアラーク東京 (1995) Silverman, J.H. and Tate, J.: Rational points on elliptic curves, Springer-Verlag, (1992)

2) GAP http://www.gap-system.org

3) Bressoud, D.M.，玉井浩訳：素因数分解と素数判定．エスアイビー・アクセス発行，星雲社発売 (2004) Bressoud, D.M.: Factorization and primality testing. Springer-Verlag, (1989)

付録　関数一覧

本文で説明していないものだけ，ごく簡単に説明する．

ワークシート上で使える関数

Function BigIntStrDump(String) As String　引き数に大きな整数の文字列を与えると，それに対応する内部表現を文字列として返す.
Function BigIntAbs(String) As String
Function BigIntNegate(String) As String
Function BigIntCompare(String, String) As Long
Function BigIntParity(String) As Long
Function BigIntSign(String) As Long
Function BigIntMax(String, String) As String　2個の大きな整数の最大値を返す.
Function BigIntMin(String, String) As String　2個の大きな整数の最小値を返す.
Function BigIntAdd(String, String) As String
Function BigIntAddLong(String, Long) As String
Function BigIntSub(String, String) As String
Function BigIntSubLong(String, Long) As String
Function BigIntMul(String, String) As String
Function BigIntMulByLong(String, Long) As String
Function BigIntMulBy10(String) As String
Function BigIntSquare(String) As String
Function BigIntPow(String, Long) As String
Function BigIntFactorial(Long) As String
Function BigIntDiv(String, String) As String
Function BigIntDivBy10(String) As String
Function BigIntDivBy2(String) As String
Function BigIntDivByLong(String, Long) As String
Function BigIntMod(String, String) As String
Function BigIntModByLong(String, Long) As String
Function BigIntMod2(String, String) As String
Function BigIntMod3(String, String) As String
Function BigIntMod4(String, String) As String
Function BigIntMod5(String, String) As String
Function BigIntMod6(String, String) As String
Function BigIntMod7(String, String) As String
Function BigIntMod8(String, String) As String
Function BigIntMod9(String, String) As String
Function BigIntRemainder(String, String) As String
Function BigIntDivAndRemainder(String, String) As String
Function BigIntRoot(String, Long) As String
Function BigIntGcd(String, String) As String
Function BigIntLcm(String, String) As String
Function BigIntModInv(String, String) As String
Function BigIntPowMod(String, String, String) As String
Function BigIntJacobi(String, String) As Long
Function BigIntModSqrt(String, String) As String
Function BigIntRandom(Long) As String
Function BigIntLshift(String, Long) As String
Function BigIntRshift(String, Long) As String

大きな整数の文字列，整数と内部表現との変換関数
Function StrClean(String) As String　引き数として与えられた大きな整数の文字列を「掃除」する.
Function StrToBigInt(String, BigInt) As Long　引き数として与えられた大きな整数の文字列を内部表現に変換する.
Function LongToBigInt(Long, BigInt) As Long　引き数として与えられた Long 型整数を大きな整数の内部表現に変換する.
Function BigIntStr(BigInt) As String　引き数として与えられた大きな整数の内部表現を数の文字列に変換する.
Function BigIntInStrDump(String, BigInt) As String
第 1 引き数として与えられた文字列と，内部表現を文字列に変換したものとを結合した文字列を返す.
Function BigIntToBin(String) As String　引き数として与えられた大きな整数の文字列を 2 進表現の文字列に変換する.
Function BinToBigInt(String) As String　引き数として与えられた 2 進数の文字列を 10 進数の文字列に変換する.

内部表現のみを処理する関数　少数の例外を除いて，BigIntIn で始まる名前を持つ.
条件判断用関数
Function BigIntInCompare(BigInt, BigInt) As Long
内部表現同士を比較する.
Function numcomp(Long, Long) As Long　上記の下請け.
Function BigIntInSign(BigInt) As Long　内部表現の符号を返す.
Function BigIntInParity(BigInt) As Long　内部表現の偶奇を返す.
Function BigIntIsOne(BigInt) As Long　内部表現が “1”

であるか.

単項演算用関数（以下，返す値は処理結果のサイズ）

Function BigIntInToZero(BigInt) As Long　内部表現を“0”にする.

Function BigIntInToOne(BigInt) As Long　内部表現を“1”にする.

Function BigIntInAbs(BigInt, BigInt) As Long　内部表現の絶対値をとり代入する.

Function BigIntInAbsSelf(BigInt) As Long　内部表現を絶対値にする.

Function BigIntInNegate(BigInt, BigInt) As Long　内部表現の符号を反転して代入する.

Function BigIntInNegateSelf(BigInt) As Long　内部表現の符号を反転する

代入，加法，減法，乗法の関数

Function BigIntInAssign(BigInt, BigInt) As Long　内部表現を代入する.

Function BigIntInAdd(BigInt, BigInt, BigInt) As Long　内部表現の和を計算する.

Function BigIntInSubtract(BigInt, BigInt, BigInt) As Long　内部表現の差を計算する.

Function BigIntInSubtractSimple(BigInt, BigInt, BigInt) As Long　上記下請け.

Function BigIntInMultiply(BigInt, BigInt, BigInt) As Long　内部表現の積を計算する.

Function BigIntInMultiplySimple(BigInt, BigInt, BigInt) As Long　上記下請け.

Function BigIntInMultiplyLong(BigInt, Long, BigInt) As Long　内部表現と Long 型整数の積を計算する.

Function BigIntInSquare(BigInt, BigInt) As Long　内部表現の 2 乗を計算する.

除法の関数

Function BigIntInDivide(BigInt, BigInt, BigInt) As Long　内部表現の商を計算する.

Function BigIntInDivideSimple(BigInt, BigInt, BigInt) As Long　上記下請け.

Function SelectFvalue(bb1 As Long, bb2 As Long) As Long　同上.

Function BigIntInDividePreop(BigInt, BigInt, BigInt, BigInt, Long) As Long　同上

Function BigIntInCalcD(BigInt) As Long　同上.

Function BigIntInCalcRes(BigInt, BigInt, Long, Long, BigInt) As Long　同上.

Function BigIntInConvQtoC(Long, BigInt, Long) As Long　同上.

Function BigIntInLShift(BigInt, Long, BigInt) As Long 内部表現を左シフトする.

Function BigIntInCalcAhT(BigInt, BigInt, Long) As Long　除法下請け.

Function BigIntInMod(BigInt, BigInt, BigInt) As Long 内部表現のモジュロを計算する.

Function BigIntInModSimple(BigInt, BigInt, BigInt) As Long　上記下請け.

Function BigIntInDivideBy1digit(BigInt, Long, BigInt) As Long　内部表現を 1 桁の数で割る.

Function BigIntInCalcRes1(BigInt, Long, Long, Long, BigInt) As Long　モジュロ下請け.

Function BigIntInDivideBy2(BigInt, Long, BigInt) As Long　内部表現を 2 で割る.

Function BigIntInDivideByLongT(BigInt, Long, BigInt) As Long　内部表現を Long 型整数で割る.

Function BigIntInDivideAndRem(BigInt, BigInt, BigInt, BigInt) As Long　内部表現の商と余りを計算する.

Function BigIntInDivideAndRemSimple(BigInt, BigInt, BigInt, BigInt) As Long　上記下請け.

その他の関数

Function BigIntInGcd(BigInt, BigInt, BigInt) As Long 最大公約数計算内部表現バージョン.

Function BigIntRootInit(String, Long) As String　冪乗根計算下請け.